UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/966,006	09/28/2001	David J. Lineman	12225.0035.NPUS00	4813

20792 7590 12/13/2005

MYERS BIGEL SIBLEY & SAJOVEC
PO BOX 37428
RALEIGH, NC 27627

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/966,006	LINEMAN ET AL.	
	Examiner	Art Unit	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *9/28/01* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed September 21, 2005 have been fully considered but they are not persuasive.

The applicant has amended independent claim 1 to recite "a security policy document in a portable representation language" that includes a "plurality of data elements for communicating the security policy" to users and "at least one data element for implementing the securing policy on computer systems in the network". The examiner has identified these limitations taught in Jacobson, see column 19, lines 19-32. Jacobson discloses of downloading a new policy when the system has determined that a policy is not effective and out of compliance with a current policy and wherein the new policy is automatically added and the software resources includes updates. It is interpreted by the examiner that the downloading is through use of a portable representation language for communicating the modified policy to the user's computer across the network and/or Internet.

It is argued that dependent claim 15 recites of "markup language" that which is a portable representation language. As argued above, Jacobson recites downloading a new policy when the system has determined that a policy is not effective and out of compliance with a current policy and wherein the new policy is automatically added and the software resources includes updates, see column 19, lines 19-32. It is interpreted by the examiner that the downloading is through use of a portable representation

language for communicating the modified policy to the user's computer across the network and/or Internet.

As per independent claim 11, it is argued the limitations "a security policy document and technical controls for implementing the security policy on at least one first computer" and "enabling creation of a security policy document.....by enabling selection of security policies from a set of options." The examiner respectfully disagrees, Jacobson recites downloading a new policy when the system has determined that a policy is not effective and out of compliance with a current policy and wherein the new policy is automatically added and the software resources includes updates, see column 19, lines 19-32.

As per independent claims 26 and 51, the applicant arguments are directed to similar limitations as are addressed above.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-56 are rejected under 35 U.S.C. 102(e) as being anticipated by Jacobson, U.S. Patent 6,735,701.

As per claim 1, it is disclosed by Jacobson of a method for managing a security policy for users in a network. A policy management program is run on a computer in communication with the network for enabling creation of a security policy document in a portable representation language using the policy management program that includes selection and inclusion in the security policy document of data elements for communicating the security policy to a user and a data element for implementing the security policy on computer systems in the network. Users on the network are enabled to view the security policy document using the plurality of data elements for communicating the security policy to users included in the security policy document and receiving electronic data relevant to user viewing of the security policy document using the policy management program (col. 2, lines 3-18; col. 10, line 57 through col. 11, line 3; and col. 19, lines 19-32).

As per claims 2 and 31, Jacobson discloses of verifying a degree of user compliance with the security policy by using the policy management program to assess the received data (col. 11, lines 3-9).

As per claim 3, Jacobson discloses of the received data includes a timestamp denoting the time a user acknowledges viewing of the security policy document (col. 20, lines 39-55).

As per claims 4 and 32, it is taught by Jacobson of the received data includes quiz results Indicative of the user comprehension of the viewed security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claims 5 and 33, the teachings of Jacobson disclose of enabling the creation of the security policy document comprises enabling selection of security policies from a set of options (col. 6, lines 47-57).

As per claims 6,12, and 34, Jacobson discloses of selecting the security policies selected a set of options reside in a library in communication with the policy management program (col. 20, lines 24-26).

As per claim 7, it is taught by Jacobson of enabling the users on the network to view the security policy document comprises enabling pre-selection of a group of users to view the security policy document (col. 5, lines 51-65).

As per claims 8 and 36, Jacobson discloses of comprising electronically providing a quiz to assess user comprehension of the viewed security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 9, Jacobson teaches of enabling the creation of the security policy document further comprises enabling creation of a quiz associated with the security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 10, it is disclosed by Jacobson of receiving data includes user responses to the quiz (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 11, Jacobson teaches of a method for managing a security policy for computers in a network. A software program is run on a second computer in communication with the network that enables the creation of a security policy document using the software program by enabling selection of security policies from a set of options. Automatically configuring the security policy document to provide technical

controls for implementing the security policy on at a first computer (col. 2, lines 3-18; col. 10, line 57 through col. 11, line 3; and col. 6, lines 47-57).

As per claims 13 and 46, Jacobson discloses that the computers operate in accordance with different operating systems (col. 1, lines 60-63 and col. 5, lines 2-7).

As per claims 14 and 47, it is taught by Jacobson that the technical controls comprise a format interpretable by at least one first computer (col. 1, lines 60-63 and col. 5, lines 2-7).

As per claims 15 and 48, Jacobson discloses that the security policy document is represented by a markup language (col. 5, lines 2-7).

As per claims 16 and 49, Jacobson teaches of distributing detect rules to a first computer (col. 8, lines 7-10).

As per claims 17 and 50, it is disclosed by Jacobson of electronically notifying an administrator when at least one first computer is out of compliance (col. 18, lines 52-54).

As per claim 18, Jacobson discloses of distributing technical controls to at least one first computer (col. 2, lines 14-19).

As per claim 19, it is taught by Jacobson of running a second software program on the first computer to allow at least one first computer to interpret the distributed technical controls (col. 2, lines 14-19).

As per claims 20 and 40, Jacobson discloses of a second software program uses metacommands to convert the technical controls into instructions interpretable by an operating system running on the first computer (col. 1, lines 60-63 and col. 5, lines 2-7).

As per claims 21 and 41, Jacobson teaches of receiving data relevant to compliance of the first computer with the one or more technical controls using the software program (col. 2, lines 14-19).

As per claims 22 and 42, it is disclosed by Jacobson of further comprising assessing the received data using a third software program (col. 2, lines 14-19).

As per claims 23 and 43, it is taught by Jacobson that the third software program comprises a security management program (col. 2, lines 14-19).

As per claims 24 and 44, Jacobson discloses of verifying a degree of compliance of the first computer with the one or more technical controls by using the software program to assess the received data (col. 5, lines 37-40 and col. 8, lines 48-60).

As per claims 25 and 45, Jacobson teaches that the received data comprises compliance score data (col. 5, lines 37-40 and col. 8, lines 48-60).

As per claim 26, Jacobson discloses of a method for managing a security policy for users and computers in a network. A software program is run on a second computer in communication with the network. A security policy document is created using the software program and automatically configuring the security policy document to create human-readable security policy document and a machine-readable security policy document containing technical controls readable by the first computer (col. 2, lines 3-18; col. 10, line 57 through col. 11, line 3; and col. 6, lines 47-57).

As per claim 27, it is taught by Jacobson of allowing the users to view the human-readable security policy document via the network (col. 5, lines 51-65).

As per claim 28, Jacobson discloses of allowing the users to view the human-readable security policy document comprises pre-selecting a group of users to view the security policy document (col. 5, lines 51-65).

As per claim 29, Jacobson teaches of electronically receiving data relevant to user viewing of the security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 30, Jacobson discloses that the received data includes a timestamp denoting the time a user acknowledged viewing the security policy (col. 20, lines 39-55).

As per claim 35, it is taught by Jacobson that the human-readable security policy document includes a quiz to test user comprehension of the security policy document (col. 5, lines 37-40 and col. 6, lines 48-60).

As per claim 38, Jacobson discloses of distributing the machine-readable security policy document to at least one first computer to implement the security technical controls thereon (col. 1, lines 60-63 and col. 5, lines 2-7).

As per claim 39, it is taught by Jacobson of running a second software program on the first computer to allow at least one first computer to interpret the distributed technical controls (col. 2, lines 14-19).

As per claim 51, Jacobson discloses of a system for managing a security policy for users and computers in a network. A first device containing a first program for creating a security policy document in both human-readable and machine-readable formats. A second device in communication with the first device and containing a second program for monitoring the security compliance of the first computer, wherein at least one first computer contains a third program for receiving the machine-readable

format of the security policy document (col. 2, lines 3-18; col. 10, line 57 through col. 11, line 3; and col. 6, lines 47-57).

As per claim 52, Jacobson teaches that the portable representation language comprises a structured data representation language (col. 19, lines 19-32).

As per claim 53, it is disclosed by Jacobson that the plurality of data elements for communicating the security policy to users includes a policy statement element, a policy commentary element, and an example element wherein the data element for implementing the security policy on computer systems in the network includes a platform control element specific to a platform type corresponding to an operating system of one of the computer systems (col. 1, lines 11-16 and col. 19, lines 19-32).

As per claim 54, Jacobson teaches of enabling creation of the security policy document comprising enabling creation of a plurality of security policy documents associated with the security policy, one of the security policy documents includes data elements for different platform types corresponding to operating systems of the computer systems in the network (col. 1, lines 11-16 and col. 19, lines 19-32).

As per claim 55, Jacobson discloses that one of the computers in the network comprise a plurality of first computers, one of which are different platform types corresponding to operating systems of the respective first computers, the method further includes a plurality of platform controls, ones of which include commands for enforcing the security policy on the different platform types corresponding to operating systems of the plurality of first computers in the network (col. 1, lines 11-16 and col. 19, lines 19-32).

As per claim 56, the teachings of Jacobson disclose that one of the first computers in the network comprises a plurality of first computers, ones of which are different platform types corresponding to operating systems of the respective first computers and wherein enabling creation of a security policy document comprises creation of a plurality of security policy documents associated with the security policy, the method further includes a platform control that includes commands for enforcing the security policy on a corresponding one of the different platform types (col. 1, lines 11-16 and col. 19, lines 19-32).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131
12/10/05

CR
December 10, 2005